

WEST Search History

[Hide Items](#)[Restore](#)[Clear](#)[Cancel](#)

DATE: Monday, November 27, 2006

Hide?	Set Name	Query	Hit Count
		<i>DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; PLUR=YES; OP=ADJ</i>	
<input type="checkbox"/>	L11	L7 and multiplex\$	30
<input type="checkbox"/>	L10	L7 and multi\$	121
		<i>DB=EPAB,JPAB,DWPI,TDBD; PLUR=YES; OP=ADJ</i>	
<input type="checkbox"/>	L8	L7	3
		<i>DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; PLUR=YES; OP=ADJ</i>	
<input type="checkbox"/>	L7	L6 and (firmware or EFI)	265
<input type="checkbox"/>	L6	(virtual machine monitor or VMM)	1305
<input type="checkbox"/>	L5	L3 and (virtual machine monitor or VMM)	9
<input type="checkbox"/>	L3	717/120,121,127,174-178.ccls.	2678
<input type="checkbox"/>	L1	20050210467	2

END OF SEARCH HISTORY

Hit List

[First](#) [Hit Clear](#)[Generate Collection](#)[Print](#)[Fwd Refs](#)[Bkwd Refs](#)[Generate OACS](#)

Search Results - Record(s) 1 through 3 of 3 returned.

☐ 1. Document ID: US 20060069534 A1

L6: Entry 1 of 3

File: DWPI

Mar 30, 2006

DERWENT-ACC-NO: 2006-261725

DERWENT-WEEK: 200627

COPYRIGHT 2006 DERWENT INFORMATION LTD

TITLE: Method for emulating host architecture in guest firmware system, involves emulating instructions executable in legacy execution mode, within guest firmware component, in native execution mode

INVENTOR: KINNEY, M D

PRIORITY-DATA: 2004US-0954622 (September 30, 2004)

PATENT-FAMILY:

PUB-NO	PUB-DATE	LANGUAGE	PAGES	MAIN-IPC
US 20060069534 A1	March 30, 2006		009	G06F017/50

INT-CL (IPC): G06F 17/50

ABSTRACTED-PUB-NO: US20060069534A

BASIC-ABSTRACT:

NOVELTY - The method involves providing a guest firmware component having a native execution mode comprising protected mode, and determining a beginning instruction executable in a legacy execution mode comprising big real mode of IA-32 architecture. The instructions executable in the legacy execution mode are emulated in native execution mode. The emulation is stopped upon detecting an end instruction executable in legacy execution mode.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

- (1) system for emulating host architecture in guest firmware system; and
- (2) machine-readable medium storing program for emulating host architecture in guest firmware system.

USE - For emulating host architecture in guest firmware system including personal computer (PC), server, mainframe computer, laptop computer, portable handheld computer, set-top box (STB), personal digital assistant (PDA), intelligent appliance and cell phone.

ADVANTAGE - Avoids performance degradation associated with transitions to virtual machine monitor, by emulating each instruction and reducing the number of expensive context shifts, thereby improving guest firmware performance.

DESCRIPTION OF DRAWING(S) - The figure shows a block diagram of the host architecture emulating system.

Full	Title	Citation	Front	Review	Classification	Date	Reference	Sequences	Attachments	Claims	KWIC	Draw Desc	Image
------	-------	----------	-------	--------	----------------	------	-----------	-----------	-------------	--------	------	-----------	-------

☐ 2. Document ID: US 20050251867 A1

L6: Entry 2 of 3

File: DWPI

Nov 10, 2005

DERWENT-ACC-NO: 2005-778335

DERWENT-WEEK: 200579

COPYRIGHT 2006 DERWENT INFORMATION LTD

TITLE: Integrity measuring method for use in computer system, involves measuring characteristic of operating system with virtual machine monitor, and storing measured characteristic in hardware protected location

INVENTOR: DARUWALA, B A; SASTRY, M R

PRIORITY-DATA: 2004US-0842670 (May 10, 2004)

PATENT-FAMILY:

PUB-NO	PUB-DATE	LANGUAGE	PAGES	MAIN-IPC
US 20050251867 A1	November 10, 2005		019	H04L009/00

INT-CL (IPC): H04L 9/00

ABSTRACTED-PUB-NO: US20050251867A

BASIC-ABSTRACT:

NOVELTY - The method involves measuring a characteristic of a virtual machine monitor, and storing the measured characteristic in hardware protected location. Another characteristic of an operating system is measured with a virtual machine monitor, in which the measuring of the lateral characteristic is initiated by the operating system. The lateral measured characteristic is stored in a hardware protected location.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

(A) an apparatus comprising a hardware protected location to store an integrity characteristic value

(B) a machine accessible medium having instructions stored to cause a machine to measure the characteristic of a virtual machine monitor.

USE - Used in a computer system for measuring the integrity of a virtual machine monitor and an operating system via secure launch.

ADVANTAGE - The method facilitates to measure the integrity of the computer system by measuring all the portions of the software and/or firmware running on the computer system, thus avoiding the exploitation by a hacker and/or a computer virus, and hence the computer systems are completely protected from outside and/or inside intrusions.

DESCRIPTION OF DRAWING(S) - The drawing shows a block diagram of a network system to test the integrity of a remote computer system via the network.

Computer system 102, 108

network 104

Network connection 106, 110

Full	Title	Citation	Front	Review	Classification	Date	Reference	Sequences	Attachments	Claims	RWMC	Draw Desc	Clip Img	Ima
------	-------	----------	-------	--------	----------------	------	-----------	-----------	-------------	--------	------	-----------	----------	-----

☐ 3. Document ID: US 20050210467 A1

L6: Entry 3 of 3

File: DWPI

Sep 22, 2005

DERWENT-ACC-NO: 2005-675545

DERWENT-WEEK: 200569

COPYRIGHT 2006 DERWENT INFORMATION LTD

TITLE: Trusted hardware sharing method in computer system, involves loading virtual machine monitor from firmware having instructions compliant with extensible firmware interface specification, to support virtual machines

INVENTOR: ROTHMAN, M A; ZIMMER, V J

PRIORITY-DATA: 2004US-0804489 (March 18, 2004)

PATENT-FAMILY:

PUB-NO	PUB-DATE	LANGUAGE	PAGES	MAIN-IPC
<u>US 20050210467 A1</u>	September 22, 2005		018	G06F009/455

INT-CL (IPC): G06F 9/455

ABSTRACTED-PUB-NO: US20050210467A

BASIC-ABSTRACT:

NOVELTY - The method involves loading a virtual machine monitor (VMM) (104) having VMM multiplexer (108) from a firmware including instructions compliant with extensible firmware interface specification, to support multiple virtual machines (VMs) in a computer system. A trusted hardware device is shared between the loaded virtual machines using the VMM multiplexer.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

(1) article of manufacture comprising computer-readable medium storing trusted hardware sharing program; and

(2) computer system.

USE - For sharing trusted hardware in trusted platform module (TPM) storing secret information such as credit card number, social security number, password, across operational environments in computer system (claimed) e.g. workstation computer, handheld or palmtop computer, personal digital assistant (PDA).

ADVANTAGE - Allows multiple operational environments to share the trusted hardware, efficiently.

DESCRIPTION OF DRAWING(S) - The figure shows a block diagram of the computer system.

virtual machine monitor 104

trusted platform module 106

virtual machine monitor multiplexer 108

trusted virtual machines 110,111,114

non-trusted virtual machines 112,113

Full	Title	Citation	Front	Review	Classification	Date	Reference	Sequences	Attachments	Claims	IMC	Draw Desc	Clip Img	Ima
------	-------	----------	-------	--------	----------------	------	-----------	-----------	-------------	--------	-----	-----------	----------	-----

Clear

Generate Collection

Print

Fwd Refs

Bkwd Refs

Generate OACS

Terms	Documents
L7	3

Display Format:

[Previous Page](#)

[Next Page](#)

[Go to Doc#](#)